Polynome

1 Faktorisierung

1.1 Definition:

K ist ein *Integritätsbereich*, wenn er folgende Eigenschaften besitzt:

1) $K = \{0, 1, \dots\}$
2) K ist kommutativ
3) $a, b \neq 0 \Rightarrow ab \neq 0$

1.2 Definition:

a heißt *Atom* in K, wenn $a \neq a_1a_2$ (a_1, a_2 sind nicht invertierbar)

1.3 Definition:

K ist ein *Bereich mit eindeutiger Zerlegung* (BEZ), wenn $\forall a \in K$ gilt: $a = a_1a_2 \dots a_r$,
wobei a_i Atome sind.
Wenn außerdem gilt: $a = b_1b_2 \dots b_s$ (b_i ebenfalls Atome), folgt, dass $r = s$

Es gilt: $b_1 = c_1a_1$, c_1 invertierbar
$b_2 = c_2a_2$, c_2 invertierbar
……….
$b_r = c_ra_r$, c_r invertierbar
und: $c_1c_2 \dots c_r = 1$

Also: $(c_1a_1)(c_2a_2) \dots (c_ra_r) = a_1a_2 \dots a_r\, c_1c_2 \dots c_r$

1.4 Definition:

Der Ingegritätsbereich R heißt *euklidisch*, wenn es eine Abb. $\varphi: R \to \mathbb{N}_0 = \{0, 1, \dots\}$ gibt und es gilt:

E.1 $\varphi(ab) \geq \varphi(a)\ \forall a,b \neq 0$ in R

E.2 $\forall a,b$, falls $b \neq 0 \Rightarrow \exists q, r \in R$: $a = bq+r$, $\varphi(r) < \varphi(b)$ oder $r = 0$

1.5 Satz:

Polynomringe sind euklidisch.

Bew.: $\varphi(a) = \deg a$

E.1: $\deg (f(x)*g(x)) \geq \deg (f(x))$

E.2: klar

=> R[x] ist euklidischer Ring

1.6 Theorem:

In einem eukl. Ring besitzen alle Elemente a, b einen ggT.

Es gilt: ggT(a, b) = au+bv , $u, v \in R$

ggT: d ist ggT, wenn gilt:

- $d|a$, $d|b$
- $d'|a$, $d'|b \Rightarrow d'|d$

Der ggT ist nicht eindeutig.

Bew.: Sei $\varphi(a) \geq \varphi(b)$. Wende E.2 wiederholt an. Nach einer endlichen Anzahl an Schritten erhalten wir das Restglied 0:

$a = bq_1+r_1 \qquad \varphi(r_1) < \varphi(b)$,

$b = r_1q_2+r_2$ $\quad \varphi(r_2) < \varphi(r_1)$,

$\dots \quad \dots \quad (1)$

$r_{n-2} = r_{n-1}q_n+r_n$ $\quad \varphi(r_n) < \varphi(r_{n-1})$,

$r_{n-1} = r_nq_{n+1}$ $\quad r_{n+1} = 0$

$\varphi(b) > \varphi(r_1) > \dots > \varphi(r_n)$ ist streng mon. fallende Folge von nichtnegativen ganzen Zahlen, die nur abbricht, wenn ein Restglied 0 ist.

Aus der ersten Gleichung sehen wir, dass r_1 die Form ax+by hat ($x, y \in R$). Durch Induktion lässt sich zeigen, dass das gleiche für r_i gilt.

Denn wenn $r_{i-1} = ax+by$ und $r_{i-2} = ax'+by'$ ist, gilt:

$r_i = -r_{i-1}q_i+r_{i-2} = -(ax+by)q_i+ax'+by' = -axq_i-byq_i+ax'+by' = a(x'-xq_i)+b(y'-yq_i)$

Also gilt: $r_n = au+bv$ $\quad (u, v\in R) \quad (2)$

r_n teilt r_n und r_{n-1}, also auch r_{n-2} und es gilt: $r_n | r_i \ \forall i$

Am Schluss erhalten wir: $r_n | b$ und $r_n | a$ (nach (1))

Also ist r_n ein gemeinsamer Teiler von a und b. Nach (2) teilt auch jeder Teiler von a und b r_n.

=> r_n ist ggT von a und b und hat die Form (2)

q.e.d.

<u>1.7 Theorem:</u> Jeder eukl. Ring ist ein BEZ.

Da F[x] euklidisch:

<u>1.8 Korollar:</u>

In jedem Körper F ist der Polynomring F[x] ein BEZ.

<u>1.9 Korollar:</u>

Sei $f = a_0+a_1x+ \dots +a_nx^n$ aus Z[x]. f hat eine rationale NS $\frac{\alpha}{\beta}$, α, β sind teilerfremd und ganzzahlig.

Dann gilt $\beta | a_n$ und wenn $\alpha \neq 0$: $\alpha | a_0$

Wenn $a_n = 1$, sind alle rat. NSTen ganzzahlig.

<u>1.10 Theorem:</u> ***(Eisensteins Kriterium)***

Sei $f = a_0+a_1x+ ... +a_nx^n$ aus Z[x]. Wenn es eine Primzahl p gibt, so dass gilt:

(i) $p \nmid a_n$,

(ii) $p | a_i$ für $0 \leq i < n$,

(iii) $p^2 \nmid a_0$,

dann ist f unzerlegbar über $\mathbb{Q}$.

<u>Bew.:</u> Angenommen, f ist zerlegbar über $\mathbb{Q}$ und daher über $\mathbb{Z}$. Sei f = gh, g und h besitzen positiven Grad und haben ganzzahlige Koeffizienten.

$g = b_0+b_1x+ ... +b_rx^r$

$h = c_0+c_1x+ ... +c_sx^s$

$r+s = n = \deg f$, $r, s > 0$

$a_0 = b_0c_0$

a_0 enthält p bis zur ersten Potenz, also ist nur entweder b_0 oder c_0 durch p teilbar.

Außerdem ist $b_rc_s = a_n$ nicht durch p teilbar => p teilt nicht b_r und p teilt nicht c_s

Also ist der erste Koeffizient von g durch p teilbar, jedoch nicht der letzte.

Sei b_i der erste nicht durch p teilbare Koeffizient von g. Dann $i > 0$ und

$a_i = b_ic_0+b_{i-1}c_1+ \dots +b_0c_i$

Wenn wir mit mod p kürzen, wird diese Gleichung zu $b_ic_0 \equiv 0 \pmod p$

Dies ist ein Widerspruch, da p b_i und c_0 nicht teilt.

Also folgt, dass f unzerlegbar ist.

q.e.d.

2 Ableitungen

2.1 Satz:

Sei α eine NST von f(x)$\in$ R[x] mit der Vielfachheit m. Dann ist die Vielfachheit von α in f'(x) m-1.

Anwendung: Sei f(x) = $(x-\alpha_1)^{k1} \dots (x-\alpha_s)^{ks}$

α_i und k_i (i =1, …, s) sind nicht bekannt.

Ziel: Konstruiere g(x) = $(x-\alpha_1) \dots (x-\alpha_s)$

Es gilt: f'(x) = $(x-\alpha_1)^{k1-1} \dots (x-\alpha_s)^{ks-1}(x-\alpha_{s+1})^{ks+1} \dots (x-\alpha_m)^{km}$

wobei $\alpha_{s+1}, \dots, \alpha_m$ NS von f'(x), aber nicht von f(x) sind

ggT (f(x), f'(x)) = $(x-\alpha_1)^{k1-1} \dots (x-\alpha_s)^{ks-1}$

g(x) = $\dfrac{f(x)}{ggT(f(x), f'(x))} = (x-\alpha_1) \dots (x-\alpha_s)$

2.2 Folgerung:

Wenn die NSTen eines Polynoms versch. Vielfachheiten besitzen, kann man die NSTen mit Hilfe des Satzes 3.1 berechnen.

Bsp.: f(x) = $(x-\alpha)^3(x-\beta)^2(x-\gamma)^1$

g(x): = $\dfrac{f(x)}{ggT(f(x), f'(x))} = (x-\alpha)(x-\beta)(x-\gamma)$ (1)

h(x): = $\dfrac{f(x)}{g(x)} = (x-\alpha)^2(x-\beta)$

i(x): = $\dfrac{h(x)}{ggT(h(x), h'(x))} = (x-\alpha)(x-\beta)$ (2)

$\dfrac{h(x)}{i(x)} = (x-\alpha)$

Aus (2) finden wir β und aus (1) γ.

2.3 Sturmische Kette

Sei $f(x) \in \mathbb{R}[x] \setminus \mathbb{R}$ ohne doppelte NSTen. Sei $[a, b] \subseteq \mathbb{R}$. Wie viele NS hat f(x) in [a, b]?

$f_0 = f$, $f_1 = f'$

Es gilt: $f_0 = q_1 f_1 - f_2$

$f_1 = q_2 f_2 - f_3$

…………

$f_i = q_{i+1} f_{i+1} - f_{i+2}$

…………

$f_{n-1} = q_n f_n - f_{n+1}$

$f_n = q_{n+1} f_{n+1}$

Bei f_{n+1} handelt es sich um eine konstante Funktion.

Man schreibe $f_0(x), f_1(x), \ldots, f_n(x), f_{n+1}(x)$ in eine Reihe.

Darunter: $f_0(a), f_1(a), \ldots, f_n(a), f_{n+1}(a)$

$f_0(b), f_1(b), \ldots, f_n(b), f_{n+1}(b)$

Sei W(x) die Anzahl der Vorzeichenveränderungen in der Reihe $f_0(x), f_1(x), \ldots, f_n(x), f_{n+1}(x)$.

2.3.1 Satz von Sturm:

Die Anzahl von NSTen von f(x) in [a, b] ist W(a)-W(b).

Bsp.: $f(x) = x^3+5x-1$, $[-10,10]$

$f'(x) = 3x^2+5 = f_1$

$f_0 = \frac{1}{3}x * f_1 - (1 - \frac{10}{3}x) \Rightarrow f_2 = 1 - \frac{10}{3}x$

$f_1 = (-\frac{9}{10}x-\frac{27}{100})*f_2-(-5-\frac{27}{100}) \Rightarrow f_3 = -5-\frac{27}{100}$

Schreibe $f_0(x)$, $f_1(x)$, $f_2(x)$, $f_3(x)$ in eine Reihe und darunter die Vorzeichen von $f_0(-10)$, $f_1(-10)$, $f_2(-10)$, $f_3(-10)$ und $f_0(10)$, $f_1(10)$, $f_2(10)$, $f_3(10)$

	x^3+5x-1	$3x^2+5$	$-\frac{10}{3}x+1$	$-5-\frac{27}{100}$	W
-10	-	+	+	-	2
10	+	+	-	-	1

W(-10)-W(10) = 2-1 = 1

Also hat f(x) im Intervall [-10,10] eine NST.

<u>3 Symmetrische Polynome</u>

<u>3.1 Definition:</u>

Sei R bel. Ring. Ein Pol. in $R[x_1, \dots, x_n]$ heißt symmetrisch, wenn es bei jeder Permutation der Unbestimmten unverändert bleibt.

Bsp. für symm. Funktionen: $x_1+x_2+ \dots +x_n$,

$x_1^2+ x_2^2+ \dots+ x_n^2$

Ist $x_1^2+ x_3^2$ symmetrisch? Wenn ja, wo?

Lösung: in $R[x_1, x_3]$

<u>3.2 Elementare symmetrische Polynome:</u>

$\sigma_1(x_1, \dots, x_n) = x_1+x_2+ \dots +x_n$

$\sigma_2(x_1, \dots, x_n) = x_1x_2+x_1x_3+ \dots +x_1x_n+x_2x_3+x_2x_4+ \dots +x_2x_n+ \dots +x_{n-1}x_n$

$\sigma_k(x_1, \dots, x_n) = \sum x_{i1}x_{i2} \dots x_{ik}$, $1\leq i_1 < i_2 < \dots < i_k \leq n$

$\sigma_n(x_1, \ldots, x_n) = x_1x_2x_3 \ldots x_n$

3.3 Viète:

$(x-\alpha_1)(x-\alpha_2) \ldots (x-\alpha_n) = x^n-\sigma_1(\alpha_1, \ldots, \alpha_n)\, x^{n-1}+\sigma_2(\alpha_1, \ldots, \alpha_n)\, x^{n-2}- \ldots +(-1)^n\sigma_n(\alpha_1, \ldots, \alpha_n)$

3.4 Satz:

Jedes symmetrische Polynom lässt sich als ein anderes Polynom, das aus elementaren symmetrischen Polynomen besteht, darstellen.

3.4.1 Beispiel.:

$$f(x) = x_1^2+x_2^2+x_3^2 = (x_1+x_2+x_3)^2-2(x_1x_2+x_1x_3+x_2x_3)$$
$$= \sigma_1^2-2\sigma_2$$

$$g(x) = x_1^3+x_2^3+x_3^3 = (x_1+x_2+x_3)^3-3(x_1x_2^2+x_1x_3^2+x_2x_3^2+x_2x_1^2+x_3x_1^2+x_3x_2^2)-6x_1x_2x_3$$
$$= \sigma_1^3-3(x_1x_2^2+x_1x_3^2+x_2x_3^2+x_2x_1^2+x_3x_1^2+x_3x_2^2)-6\sigma_3$$

gesucht: Algorithmus, mit dem das blau Geschriebene in elementaren symmetrischen Polynomen darstellbar ist

3.4.2 Algorithmus:

Sei f(x) symmetrisch.

1) Bestimmen des Hauptmonoms (nach lexikographischer Anordnung)

Sei $f(x) = x_1^{k1}\, x_2^{k2} \ldots x_n^{kn}+ \ldots$

Betrachte $\sigma_1^{k1-k2}\sigma_2^{k2-k3} \ldots \sigma_{n-1}^{kn-1-kn}\sigma_n^{kn}$

Lemma: $HM(\sigma_1^{k1-k2}\sigma_2^{k2-k3} \dots \sigma_{n-1}^{kn-1-kn}\sigma_n^{kn})$

$= (HM((\sigma_1))^{k1-k2}(HM((\sigma_2))^{k2-k3} \dots (HM((\sigma_n))^{kn}$

$= x_1^{k1-k2}(x_1x_2)^{k2-k3} \dots (x_1x_2 \dots x_{n-1})^{kn-1-kn}(x_1x_2 \dots x_n)^{kn}$

$= x_1^{k1}x_2^{k2} \dots x_n^{kn}$

2) Dann ist $g(x) = f(x)- \sigma_1^{k1-k2}\sigma_2^{k2-k3} \dots \sigma_{n-1}^{kn-1-kn}\sigma_n^{kn}$

Es gilt: $HM(g(x)) < HM(f(x))$

3.4.2.1 Beispiel:

$f(x) = x_1x_2^2+x_1x_3^2+x_2x_3^2+x_2x_1^2+x_3x_1^2+x_3x_2^2$

1) HM ist $x_2x_1^2 \Rightarrow k_1 = 2, k_2 = 1, k_3 = 0$

Betrachte $\sigma_1^{k1-k2}\sigma_2^{k2-k3}\sigma_3^{k3} = \sigma_1^1\sigma_2^1\sigma_3^0 = (x_1+x_2+x_3)(x_1x_2+x_1x_3+x_2x_3)$

$= x_1^2x_2+x_1^2x_3+x_1x_2x_3+x_1x_2^2+x_1x_2x_3+x_2^2x_3+x_1x_2x_3+x_1x_3^2+x_2x_3^2$

$= x_1^2x_2+x_1^2x_3+x_1x_2^2+x_2^2x_3+x_1x_3^2+x_2x_3^2+3x_1x_2x_3$

2) Dann gilt:

$g(x)= f(x)-\sigma_1\sigma_2$

$= x_1x_2^2+x_1x_3^2+x_2x_3^2+x_2x_1^2+x_3x_1^2+x_3x_2^2-(x_1^2x_2+x_1^2x_3+x_1x_2^2+x_2^2x_3+x_1x_3^2+x_2x_3^2+3x_1x_2x_3)$

$= -3x_1x_2x_3 = -3\sigma_3$

f lässt sich also darstellen als:

$f(x) = \sigma_1\sigma_2-3\sigma_3$